(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 January 2001 (04.01.2001)

PCT

(10) International Publication Number
WO 01/01361 A1

(51) International Patent Classification[7]: G07F 19/00, G06F 17/60

(21) International Application Number: PCT/GB99/02017

(22) International Filing Date: 28 June 1999 (28.06.1999)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: BARCLAYS BANK PLC [GB/GB]; 54 Lombard Street, London EC3P 3AH (GB).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: ALEXANDER, Roger, Keith [GB/GB]; 23 The Glebe, Badby, Daventry, Northamptonshire NN11 3AZ (GB).

(74) Agents: CROSS, James, P., A. et al.; R G C Jenkins & Co, 26 Caxton Street, London SW1H 0RJ (GB).

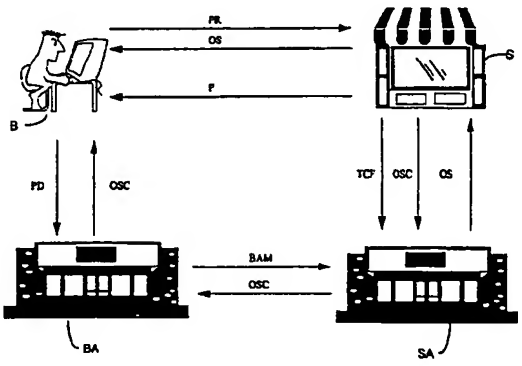
(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SECURE TRANSACTION SYSTEM



(57) Abstract: In an electronic transaction system, a buyer (B) initiates a purchase from a seller (S), which sends an offer to sell (OS) to the buyer (B) over the Internet. The buyer (B) sends payment details (PD) over the Internet to a buyer authenticator (BA), which authenticates the identity of the buyer (B) and sends a buyer authentication message (BAM), over a secure network to a seller authenticator. From the contents of the buyer authentication message (BAM), the seller authenticator (SA) identifies the seller (S) and sends the offer to sell message (OS) to the seller (S). The seller (S) checks whether the offer to sell message matches that originally sent to the buyer, and if so sends an offer to sell confirmation (OSC) to the seller authenticator (SA), where the message is forwarded to the buyer authenticator (BA) and thence to the Buyer (B). Fulfilment (F) of the order is initiated and the seller sends a transaction confirmation to the seller authenticator (SA). The system uses the authenticators as intermediaries to establish a virtual trust domain between buyer and seller. Security is increased by requiring that both buyer and seller confirm the existence of the transaction to other parties. A modification is also disclosed in which the buyer authenticator calculates any tax due on the delivery of the order, and obtains the buyer's agreement to pay this tax before the transaction can proceed.

WO 01/01361 A1

SECURE TRANSACTION SYSTEM

Technical Field

The present invention relates to a secure transaction system, particularly for use over a public network, and particularly but not exclusively for processing payment transactions.

Background Art

There has been considerable activity in the field of Internet-based electronic commerce to develop appropriate standards for secure electronic transactions ('e-commerce'). The standards aim to provide:

privacy of information - such that the content of a transaction cannot be read by a third party;

data integrity - to ensure that the content cannot be changed during transmission across the Internet;

authentication of the parties to the transaction - to avoid fraudulent activity by the buyer and/or seller; and

non-repudiation of the transaction - to provide evidence of the transaction should it subsequently be disputed by one of the parties.

Much activity has been focussed on the development of SET (Secure Electronic Transactions), a protocol designed to protect Visa and Mastercard transactions. defined in the 'Secure Electronic Transaction (SET) Specification', 23 February 1996. However, SET is recognised as being difficult to implement and expensive to develop and support. Interoperability of components from different suppliers continues to give cause for concern. Moreover, the portability and inherently insecure nature of software-based solutions are recognised as a limitation to the widespread adoption of the protocol.

Retailers already active in e-commerce find it difficult to understand the value of adopting SET. Many are content with SSL (Secure Sockets Layer, defined in 'The SSL Protocol Version 3.0', March 1996) and are not prepared to change their approach without incentives from financial institutions. The latter have meanwhile not developed a business case for the adoption of SET. SET therefore seems unlikely to be used extensively, at least in the short term.

The current e-commerce model, as shown in Figure 1, replicates that used for card purchases in a physical environment in which a buyer is physically present at the seller's premises, or conducts a transaction with the seller over the telephone. The buyer B sends a purchase request PR to the seller S. for example by selecting a particular item from a web page hosted on behalf of the seller S, and receives purchase information PI from the seller, confirming the price and identity of the item selected and prompting the buyer for payment details. The buyer B submits the payment details PD, such as card and buyer details, to the seller S.

The seller S then submits an Authorization Request AR to an Acquirer A, such as the seller's bank, who passes the Authorization Request AR to the Issuer I of the card used by the buyer B in the transaction. The Issuer checks that the card and buyer details contained in the Authorization Request AR are correct and that the payment is within the buyer's authorized limit. If the payment is authorized, the Issuer sends an acceptance message ACC to the Acquirer A, who passes the acceptance message ACC to the seller S. The seller S then fulfils F the transaction, by delivering the item ordered and/or issuing confirmation that the order has been accepted and the payment will be debited from the buyer's account. The seller S then sends a transaction confirmation message TCF to the Acquirer A.

In considering security issues, it is important to differentiate between traditional fraud perpetrated via the Internet and 'Internet Fraud'. new types of

fraud specific to the Internet, which cannot be perpetrated over other channels or can be undertaken far more easily over the Internet. In an e-commerce transaction, the buyer B interacts with the seller S over the Internet, which gives rise to security concerns. One concern is that account-related information passes through a number of intermediary servers between the buyer B and the seller S in a way that cannot in general be controlled. Retention of the account details by intermediary servers or within the seller's server can be used for the purposes of fraud. Another concern is fraudulent activity by buyers, in which stolen or invalid account details are given, and fraudulent activity by sellers, in which payment is obtained without the transaction being fulfilled. Until fears of fraudulent sellers can be overcome. buyers will not widely accept such a transaction model. Likewise. sellers need to be reassured against fraudulent activity by buyers B. For example, there is a rising incidence of 'Internet Fraud' in which the fulfilment stage F itself takes place over the Internet, such as the downloading of software from a 'download shop'.

The document EP-A-0 779 587 discloses a payment settlement system for on-line shopping in which the user selects an item from an on-line shop over the Internet, but sends credit card data via a separate settlement network to a 'service centre' which sends the payment details to an 'approval centre' (e.g. a card issuer) for authorization and notifies the operator of the on-line shop if the payment has been authorized. The service centre also sends the order data to the operator, so that the order can be fulfilled. While such a system avoids the transmission of account details over the Internet, it is difficult to see what advantage is gained over the well-known method of identifying products over the Internet, and subsequently sending credit card details directly to the relevant shop by telephone or fax. Moreover, the system is still open to fraud, since there is apparently no means of establishing trust between the user and the shop, and is vulnerable to replay attacks.

A further problem associated with Internet shopping is that of import taxes, such as duty and value added tax (VAT). An on-line shop may not have a warehouse within the same country or economic area as the buyer and therefore the ordered goods have to be imported by the buyer, usually by mail or courier. The buyer is therefore liable to pay import taxes, which vary according to the country as well as the type of goods, so that the buyer does not usually know the tax due and cannot readily judge the total cost of the purchase. Frequently, the cost advantage of shopping over the Internet is cancelled by import taxes, so ideally the buyer would like to know the total cost before proceeding with the transaction. Moreover, the goods may be impounded or delayed by customs. If the goods are not detected by customs, the import taxes are often not paid at all by the buyer.

Statement of the Invention

In accordance with one aspect of the present invention, there is provided a system for conducting a payment transaction between a paying party and a receiving party, in which transaction identification information is transmitted from one of the parties to the other. The paying party transmits an instruction to pay to an intermediary, and the transaction identification information is transmitted from the party which receives it to the intermediary, which then transmits the transaction identification information to the party which originally transmitted the transaction identification information. The payment is not allowed to proceed unless the transaction identification information as received from the intermediary matches that originally transmitted. In this way, the existence of the current transaction is confirmed by both parties before the payment is allowed to proceed, preventing 'replay' fraud in which information from a previous transaction is replayed by the receiving party, or by a party intercepting the previous transaction, to trigger repeat payments.

To allow the intermediary to transmit the transaction identification information to the originating party, the intermediary is provided with information identifying the originating party in the current transaction. Therefore, the intermediary is able to check the identity of the originating party and only to transmit the transaction identification information to the originating party if that party is authorised to use the system. This aspect also prevents bogus on-line shops from obtaining account information or payment by passing themselves off as trusted shops. If the bogus shop identifies itself as a trusted shop and sends this information to the buyer, this identification information will be transmitted by the buyer to the intermediary, which then contacts the trusted shop. The trusted shop has no record of the current transaction and therefore prevents the payment being made.

According to another aspect of the present invention, there is provided a payment transaction system for conducting a payment transaction between a buyer and a seller, in which a buyer authenticator, in communication with the buyer, verifies the authenticity of the buyer, a seller authenticator, in communication with the seller, verifies the authenticity of the seller, and payment instructions for the transaction are transmitted from the buyer authenticator to the seller authenticator. This system greatly simplifies the establishment of a trust relationship between the buyer and the seller, by reducing the problem to that of establishing trust between the buyer authenticator and the seller authenticator. The authenticators may each serve a large number of buyers and sellers, so that the number of possible connections between buyer authenticators and seller authenticators over which trust must be established is greatly reduced. Furthermore, whereas the buyer must be allowed to communicate via the Internet in order to encourage acceptance of the system, the buyer and seller authenticators can be interconnected by a more secure network, such as a circuit-switched network. The trust relationship between buyer and buyer authenticator, and between

seller and seller authenticator can be easily established by pre-registration, whereas direct pre-registration between buyers and sellers is not feasible. Hence, this four-party model breaks the trust problem of the huge number of potential connections between buyers and sellers into the much more manageable number of connections between each buyer authenticator and its registered buyers, between each buyer authenticator and each seller authenticator, and between each seller authenticator and its registered sellers. Thus, the certification hierarchy of SET can be replaced by, for example, different secret keys for each connection, the secret keys being set during preregistration or by separate communications between authenticators.

According to a further aspect of the present invention, there is provided a system for conducting a purchase transaction between a buying party and a selling party, in which information identifying the goods to be purchased is transmitted to an intermediary, which calculates an additional amount due to a party other than the selling party dependent on the identity of the goods to be purchased and preferably the destination to which the goods are to be delivered. Preferably, the additional amount is indicated to the buying party and the purchase transaction is only allowed to proceed if the buying party confirms that the additional amount should be paid. Preferably, the intermediary automatically triggers the payment of the additional amount if the purchase transaction is allowed to proceed. One advantage of this aspect is that the additional amount, such as an import tax, is automatically paid so that delivery can proceed without delay or tax evasion. Another advantage is that the buyer knows the total payment due before entering into the purchase transaction.

Brief Description of the Figures

Specific embodiments of the present invention will now be described with reference to the accompanying drawings, in which:

Figure 1 is a diagram of the stages in a conventional payment transaction;

Figure 2 is a diagram of the stages in a payment transaction system in an embodiment of the present invention;

Figure 3 is a diagram showing the technical means by which the transaction of Figure 2 may be conducted;

Figure 4 is a diagram of the relationships of trust between the parties in the system of Figure 2;

Figure 5 is a diagram showing a virtual trust relationship between buyer and seller as a result of the relationships shown in Figure 4; and

Figure 6 is a diagram showing a protocol for calculating and paying import taxes, which can be applied to the protocol shown in Figure 2.

Modes for Carrying Out the Invention

Transaction Protocol

An embodiment of the present invention will now be described with reference to Figures 2 and 3, which show a sequence of interactions for processing a payment transaction. As in the conventional system, the buyer B operates a buyer terminal BT, which may be a general purpose computer or dedicated Internet terminal running TCP/IP and Internet browser software, and browses a website hosted on a seller's server SS, via the Internet. The Internet browser software may include a 'plug-in', or a discrete application may be run, which implements the transaction protocol of this embodiment, as performed on the buyer's terminal BT. The buyer B indicates a desire to purchase one or more items, such as goods or services, by selecting an item displayed within the web browser, which sends a Purchase Request message PR via the Internet to the seller S.

In response to the Purchase Request Message PR, the seller S then sends to the buyer B, over the Internet I, an Offer to Sell message OS,

including details of the intended purchase and the seller's identity, preferably in a form which can be verified later by the seller but is difficult to reproduce by another party. The Offer to Sell message includes a seller agreement reference identifying a previously concluded agreement between the seller S and the seller authenticator SA.

On receipt of the Offer to Sell information OS, the software on the buyer's terminal BT enters an authentication process with the buyer B. This process may comprise reading a smartcard carrying account details and identification information of the holder of the card, and inputting a PIN and/or biometric information from the buyer B. This information may be digitally signed, for example by generating and encrypting a hash of the information, using a key stored on the smart card and not known to the buyer. The buyer B may also digitally sign the Offer to Sell information. The signed information and Offer to Sell information are sent as payment details PD over the Internet I to a buyer authenticator BA, which may be a server BAS operated by the buyer's bank.

The buyer authenticator BA checks the details of the buyer B contained within the payment details PD, for example by validating the signature of the Offer to sell information using a key previously assigned to the buyer B when issuing the smartcard, and checking that the PIN and/or biometric information are correct. As an alternative, the PIN and/or biometric information may be validated at the buyer's terminal BT against a PIN or biometric information stored on the smart card. If the PIN and/or biometric information do not match after a predetermined number of attempts, the software on the buyer's terminal BT may terminate the transaction and optionally send a message to the buyer authenticator BA indicating a failed attempt to use the smartcard.

In either case, if the buyer is authenticated, but not otherwise, the buyer authenticator BA sends a buyer authentication message BAM via a

secure channel to a seller authenticator SA, which may be a server SAS operated by the seller's bank. The secure channel may be a circuit switched connection via a private network PN, or via a public network such as a PSTN or ISDN. The buyer authentication message BAM includes the Offer to Sell information, payment information, and a flag indicating whether the buyer has been authenticated. The seller authenticator SA checks the seller agreement reference in the Offer to Sell information and, if this reference corresponds to seller agreement recognised by the seller authenticator SA, sets up a communications channel to the seller identified by the seller agreement reference using pre-stored connection details. For example, where the connection to the seller's server SS is via a leased line, the seller authenticator routes all messages intended for the seller through that leased line. Where the connection is a dial-up connection, the seller authenticator SA dials a number pre-stored in the seller agreement record indicated by the seller agreement reference.

The seller authenticator forwards the Offer to Sell Information to the seller, for example via a leased line connection LL, or the Internet I. The Offer to Sell information is digitally signed by the seller authenticator. This signature may be generated by a secret key known only to the seller S to which the Offer to Sell information is to be sent, and established during pre-registration of the seller with the seller authenticator.

The seller verifies the seller authenticator's signature and checks whether the Offer to Sell Information was indeed originated by itself in a current transaction. For example, the seller may include a unique transaction number in the Offer to Sell information, generated in a sequence which is difficult to predict by another party. The unique transaction number and other information unique to the current transaction and included in the Offer to Sell information may be encrypted using a secret key stored in the seller's server SS.

If the seller verifies the seller authenticator's signature and that the transaction is current, it sends an Offer to Sell Confirmation message OSC via the Internet I back to the seller authenticator SA. The Offer to Sell Confirmation message is forwarded to the buyer authenticator via the secure channel and thence to the buyer B via the Internet I. At each stage, the recipient party verifies the identity of the sender of the Offer to Sell Confirmation Message, for example by verifying a digital signature by the sending party of the Offer to Sell Confirmation message. The Offer to Sell Confirmation Message includes information derived from the Offer to Sell Information, which is unique to the current transaction, so that replays of Offer to Sell Confirmation Messages can be detected. The seller S then performs a fulfilment operation F with the buyer, by initiating the delivery of the purchased item or items to the buyer B or by delivering the item over the Internet in the case where the item purchased is software, data, or some interactive service such as advice or support. The seller also sends a transaction confirmation TCF to the seller authenticator SA, which triggers the clearing and settlement of the payment in the transaction through conventional channels, as currently used by issuers such as Mastercard (RTM) and Visa (RTM).

Trusted Domains

One of the bases of the SET protocol is the creation of a trust hierarchy based on public key certificates. This requires the signatory of a public key certificate to be trusted by the authenticating party, or for the authenticity of the signatory to be established from one or more higher levels of public key certificate, the highest level of which is signed by a trusted party. The SET trust hierarchy is necessary because the payment transaction is conducted between parties having no pre-existing trust relationship.

In contrast, the protocol of the embodiment described above controls security through a chain of trust comprising trust domain d1 between the buyer B and the buyer authenticator BA, trust domain d2 between the buyer authenticator BA and the seller authenticator SA, and domain d3 between the seller authenticator SA and the seller S, as represented by Figure 4. An appropriate level of security can be applied independently to each link, using a security technique suitable for that trusted domain. Examples of such techniques have been given above, but other techniques may be substituted within the abilities of the skilled person.

The buyer B has a pre-existing relationship with the buyer authenticator BA, for example through a registration procedure. The buyer authenticator's server may maintain an electronic wallet or personal electronic data store (PEDS) for the buyer, so that the account details of the buyer are stored at the buyer authenticator Server BAS and are not transmitted over the Internet from the buyer to the buyer authenticator BA. Instead, the buyer authenticator BA transmits the account details of the buyer B to the seller authenticator only when authorized to do so by the buyer.

The buyer may be issued with a smart card storing encryption keys and/or algorithms by means of which an on-line authentication protocol is conducted with the buyer authenticator BA. The buyer authenticator BA is required to underwrite the transaction sent to the seller against fraud by the buyer, and therefore it is the responsibility of the buyer authenticator to verify the identity of the buyer.

The trusted domain d2 between the buyer authenticator BA and the seller authenticator SA operates through an international payment system such as that used between banks under the Visa or Mastercard systems, or the Global Trust system as announced on 21 October 1998 in New York by ABN AMRO, Bank of America, Bankers Trust, Barclays Bank, Chase Manhattan, Citibank, Deutsche Bank and Hypo Vereinsbank, and CertCo, now known as

'Identrus' ™ and joined by two further members, Canadian Imperial Bank of Commerce and Sanwa Bank. This type of trusted domain operates through an intermediary which certifies all buyer and seller authenticators using a standard certified identity.

The seller authenticator SA has a pre-existing relationship with the seller S, for example by pre-registration. The seller authenticator SA guarantees the authenticity of the seller S and accepts at least some liability for transactions with that seller.

Through the use of the overlapping trusted domains d1, d2 and d3, there exists a virtual trusted domain D between the buyer B and the seller S, as illustrated in Figure 5.

The above described embodiment achieves several advantages over the SET protocol:

- account information is not passed from the buyer B to the seller S across an open network (e.g. the Internet)

- the amount of account information transmitted from the buyer B to the buyer authenticator BA across the open network (e.g. the Internet) may be further limited by the use of electronic wallets at the buyer authenticator's server

- the seller S only gains access to account information of the buyer once both the buyer B and the seller S have been authenticated, in the Offer to Sell information

- hashing techniques are used to protect the integrity of the data

- mutual authentication of the buyer and seller is achieved through the use of trusted domains

- Authentication of the buyer allows subsequent repudiation issues to be resolved

- Security issues are simplified by the use of trusted domains

- payment guarantee can be provided prior to virtual fulfilment.

The above transaction system also allows buyer authenticators BA and seller authenticators SA flexibility in their respective relationships with buyers B and sellers S. Seller authenticators can provide financial incentives to sellers S to encourage them to trade through the system, and buyer authenticators can create whatever transaction protocols and business processes are necessary to alleviate the buyers' concerns about security. The transaction system is based around the position of trust that financial institutions, as buyer authenticators and seller authenticators, enjoy with their customers as buyers and sellers, and among themselves, by the use of existing or planned trust systems.

Tax Calculation

An additional protocol which may be added to the protocol shown in Figure 2 will now be described with reference to Figure 6. With the Offer to Sell message OS, the seller S transmits to the buyer B Classification of Goods information CG and Country of Export information CE. The Classification of Goods information CG identifies the goods to be sold in the transaction according to a standard classification, such as the Harmonized System (HS) classification used by customs authorities. If multiple different types of goods are being purchased, falling under different classifications, the Classification of Goods message lists the value of goods to be purchased under each classification. The Country of Export information CE identifies the country or tax jurisdiction from which the goods will be exported. The buyer B includes the Classification of Goods and Country of Export information in the Payment Details message PD.

The buyer authenticator BA stores, for example on its server BAS, a database of import tax rates due on different classifications of goods, as a function of the country of export and the country of import. The buyer

authenticator also has available the address to which the goods will be delivered; this may be the address of the buyer B as registered against the account from which the payment will be made, and may be provided in the payment details PD or be pre-stored at the buyer authenticator Server BAS. Alternatively, if the goods are ordered as a gift for delivery to another address, that address is supplied by the buyer B. From this, the buyer authenticator BA derives the country or jurisdiction to which the goods are to be delivered. The buyer authenticator BA then calculates the import tax payable by the buyer according to the applicable tax rate retrieved from the database, using the identifications of the country of import, the country of export, and the value and classification of the goods. The import tax information TI is transmitted from the buyer authenticator BA to the buyer B. The software running on the buyer's terminal BT displays the import tax information and asks the buyer B whether to proceed with the transaction. If the buyer confirms this, a tax confirmation message TC is sent from the buyer to the buyer authenticator.

Later during the transaction the buyer authenticator BA, in response to receipt of the Offer to Sell Confirmation OSC, initiates a payment TP of the import tax due from the buyer's account to the account of the customs authority responsible for collecting import taxes for the country of delivery of the ordered goods. In this way, the payment of import taxes is automated and the delivery of goods should not be delayed by customs authorities. However, the taxes are only paid with the consent of the buyer, and once the transaction has been confirmed by both the buyer B and the seller S.

As one possible alternative, the buyer B may provide sufficient information to the buyer authenticator BA to allow the tax information TI to be sent back to the buyer B, before the rest of the Payment Details PD are sent to the buyer authenticator. This provides greater comfort to the buyer that the

payment for the transaction and for any taxes due cannot be made until the buyer B has confirmed that the taxes are acceptable.

As another alternative, the buyer B only transmits the Classification of Goods information CG and the Country of Export information CE to the buyer authenticator BA once the buyer B has received the Offer to Sell Confirmation OSC. The protocol then proceeds, with the Tax Information TI being sent to the buyer B and the buyer replying with the Tax Confirmation TC, in response to which the buyer authenticator BA initiates payment of the taxes. This alternative allows the buyer B to proceed with the transaction without paying the taxes automatically, and may therefore be more attractive to the buyer B.

It will be understood that some types of goods are not subject to import taxes in some countries, and some countries do not impose import taxes on any imports from certain other countries, such as countries within the European Union. If no tax is payable, the protocol may proceed without requiring a tax confirmation TC from the Buyer B, and optionally without sending the tax information TI to the Buyer.

Although the above protocol has been described with reference to taxes, it could alternatively be used in situations where certain taxes are included in the price charged by the seller, but these taxes can be reclaimed by the Buyer. In that case, the Buyer Authenticator may initiate a claim from the relevant tax authority for a tax refund to be paid to the buyer's account.

Alternative Protocols

In the transaction described above, the payment details are submitted for payment processing by the seller authenticator, once the transaction confirmation is received. However, the payment details may be submitted for processing by other parties. For example, the seller S may submit the payment details for processing directly, rather than through the seller authenticator SA.

Furthermore, the payment may be pre-authorised before fulfilment F takes place. For example, the buyer authenticator BA may be the issuer of the smart card used by the buyer. In that case, the buyer authenticator BA confirms that the use of the card is authorised, in the buyer authentication message BAM. Payment processing is then triggered by the offer to sell confirmation OSC being received by the buyer authenticator BA. Alternatively, the transaction confirmation TCF may be forwarded from the seller authenticator to the buyer authenticator BA, whereby the payment processing is triggered.

In an alternative form of pre-authorisation, the seller authenticator may request authorisation for the payment from the card issuer and terminate the transaction protocol if authorisation is denied. For example, on receipt of the offer to sell message, the seller authenticator may submit the payment details to the card issuer, and only forward the offer to sell message to the seller if the payment amount is authorized by the issuer.

In the above described embodiments, the Offer to Sell message OS is generated by the seller S and returned to the seller for confirmation via the buyer authenticator BA and the seller authenticator SA. Alternatively, the seller S may send the information content of the purchase request PR to the seller authenticator SA, which information is passed to the buyer authenticator and then returned to the buyer B, the transaction not being allowed to proceed to payment and delivery until the buyer has confirmed that the Purchase Request PR is current. However, the buyer must still send the payment details PD to the buyer authenticator BA and thence to the seller authenticator SA, so that the protocol requires a greater number of separate information transfers to take place.

The functions of the buyer authenticator BA and the seller authenticator SA may be combined into a single party, so that the buyer Authentication Message BAM is an internal message which is not transmitted

over external communications links. This eventuality is possible in the above described embodiments, if coincidentally the buyer B and the seller S are using the services of the same bank as their respective authenticators. Alternatively, the protocol may be designed so that the buyer authenticator BA and the seller authenticator SA must be the same party. Although this three-party arrangement may still benefit from other aspects of the transaction protocol, the centralised authenticator would then need to establish trust relationships with a very much larger number of users, both as buyers and sellers, than would the separate buyer authenticators BA and seller authenticators SA. Moreover, the buyers and sellers could not rely on their existing relationships with their banks, but would have to register with the centralized authenticator as a new organisation.

The above protocol is advantageously applied to a payment transaction, but could be applied to a transaction in which certain other types of agreement are concluded between two parties. For example, the buyer may instead be entering into a contract to buy a property, such as a house, from the seller. The buyer authenticator, on request by the buyer, provides details of the financial position of the buyer to the seller authenticator together with details of the cost of the property. The seller authenticator checks from these details as to whether the buyer is likely to be able to pay for the property, and sends a simple confirmation or denial message, together with identification of the current transaction, to the seller. In this way, the seller can check that the buyer's financial status is sufficient without the buyer having to supply detailed financial status information directly to the seller, which would put the seller in an advantageous position in negotiating the price. Moreover, fraudulent attempts to obtain financial information about the buyer can be prevented, in the same way as access to account information.

CLAIMS

1. A method of conducting an electronic transaction between a first party and a second party, including:

initiating the transaction between the first and second parties,

in response to initiation of the transaction, generating by the second party transaction identification information substantially unique to the initiated transaction,

transmitting the transaction identification information from the second party to the first party,

transmitting the transaction identification information from the first party to an intermediary,

transmitting the transaction identification information from the intermediary to the second party,

comparing, by the second party, the transaction identification information received from the intermediary with the transaction identification information as generated by the second party in a current transaction, and

preventing the transaction from proceeding to completion if the transaction identification information received from the intermediary does not match the transaction identification information generated by the second party.

2. A method as claimed in claim 1, wherein the intermediary identifies the second party, and selectively transmits the transaction identification information to the second party, in response to said transaction identification information.

3. A method as claimed in claim 1 or 2, wherein the second party determines whether the transaction identification information received from

the intermediary matches the transaction identification information generated by the second party and transmits to the intermediary a transaction confirmation message if said determining step yields a positive result.

4. A method as claimed in any preceding claim, wherein the intermediary comprises a first party intermediary arranged to communicate with the first party and a second party intermediary arranged to communicate with the second party, the first party intermediary being connected to the second party intermediary via a communications network.

5. A method as claimed in any preceding claim, wherein the first party is a buying party and the second party is a selling party in an electronic payment transaction.

6. A method as claimed in claim 5 when dependent on claim 3, wherein the intermediary initiates payment in the transaction in response to said transaction confirmation message.

7. A method as claimed in claim 5 or claim 6, further including initiating delivery by the second party in fulfilment of the transaction if the transaction identification information received from the intermediary matches the transaction identification information generated by the second party.

8. A method of conducting an electronic transaction between a first party and a second party, including:

connecting the first party to the second party and initiating the transaction via a first communications channel;

transmitting transaction information from the first party to the first party authenticator and verifying the identity of the first party at the first party authenticator via the second communications channel,

transmitting the transaction information from the first party authenticator to a second party authenticator via a third communications channel, and

connecting the second party authenticator to the second party via a fourth communications channel, whereby the identity of the second party is verified by the second party authenticator,

wherein the transaction is prevented from proceeding to completion unless the identity of the first party is verified by the first party authenticator and the identity of the second party is verified by the second party authenticator.

9. A method as claimed in claim 8, wherein the identity of the first party is verified by transmitting first party identification information from the first party to the first party authenticator and comparing the first party identification information with identification information stored by the first party authenticator.

10. A method as claimed in claim 8 or claim 9, wherein the identity of the second party is verified by the second party authenticator by comparing at least part of said transaction information with second party identification information stored by the second party authenticator.

11. A method as claimed in claim 8 or claim 9, wherein the identity of the second party is verified by the second party authenticator by receiving second party identification information over the fourth communications channel and

comparing said second party identification information with information stored at the second party authenticator.

12. A method as claimed in any one of claims 8 to 11, wherein said first party authenticator stores account information relating to the first party and transmits said account information to the second party authenticator if the identity of the first party is verified, the account information not being transmitted by the first party to the first party authenticator during the current transaction.

13. A method as claimed in any one of claims 8 to 12, wherein said third communications channel is set up over a network.

14. A method as claimed in any one of claims 8 to 13, wherein the first communications channel is carried by a public packet-switched network.

15. A method as claimed in claim 14, wherein the second communications channel is carried by the public packet-switched network.

16. A method as claimed in any one of claims 8 to 15, wherein said transaction is an electronic payment transaction, and payment is initiated by one of the first part authenticator and the second party authenticator.

17. A method of conducting a goods ordering transaction between an ordering party and a supplying party, including:

transmitting, from the supplying party to the ordering party, supply identification information relating to the supply of the goods in the transaction,

transmitting, from the ordering party to an intermediary, said supply identification information, and

calculating, at said intermediary, an amount due to a party other than the supplying party on the basis of the supply identification information.

18. A method as claimed in claim 17, including transmitting amount information identifying said amount to said ordering party.

19. A method as claimed in claim 17 or claim 18, further including:

initiating payment of said amount to said party other than said supplying party.

20. A method as claimed in claim 19 when dependent on claim 18, wherein said payment is only initiated on confirmation by the ordering party.

21. A method as claimed in claim 19 or claim 20, wherein said payment is initiated by said intermediary.

22. A method as claimed in claim 21 when dependant on claim 20, wherein the ordering party transmits a confirmation message to the intermediary if said payment is confirmed, and the intermediary initiates payment of the amount in response to said confirmation message.

23. A method as claimed in any one of claims 17 to 22, further including transmitting a payment authorization message, relating to a payment from the ordering party to the supplying party, from the ordering party to the intermediary.

24. A method as claimed in claim 23 when dependent on claim 22, wherein the intermediary prevents said payment from the ordering party to the supplying party unless the confirmation message is received from the ordering party.

25. An electronic transaction system arranged to perform the method according to any preceding claim.

26. Electronic communications apparatus arranged to perform the method steps carried out by the first party in the method as claimed in any one of claims 1 to 16.

27. Electronic communications apparatus arranged to perform the method steps carried out by the second party in the method as claimed in any one of claims 1 to 16.

28. Electronic communications apparatus arranged to perform the method steps carried out by the intermediary in the method as claimed in any one of claims 1 to 7 when not dependent on claim 4, or by one of the first party intermediary and the second party intermediary in the method as claimed in claim 4, or as claimed in claim 5 or claim 7 when dependent on claim 4.

29. Electronic communications apparatus arranged to perform the method steps carried out by the first party authenticator in the method as claimed in any one of claims 8 to 16.

30. Electronic communications apparatus arranged to perform the method steps carried out by the second party authenticator in the method as claimed in any one of claims 8 to 16.

31. Electronic communications apparatus arranged to perform the method steps carried out by the ordering party in the method as claimed in any one of claims 17 to 24.

32. Electronic communications apparatus arranged to perform the method steps carried out by the supplying party in the method as claimed in any one of claims 17 to 24.

33. Electronic communications apparatus arranged to perform the method steps carried out by the intermediary in the method as claimed in any one of claims 17 to 24.

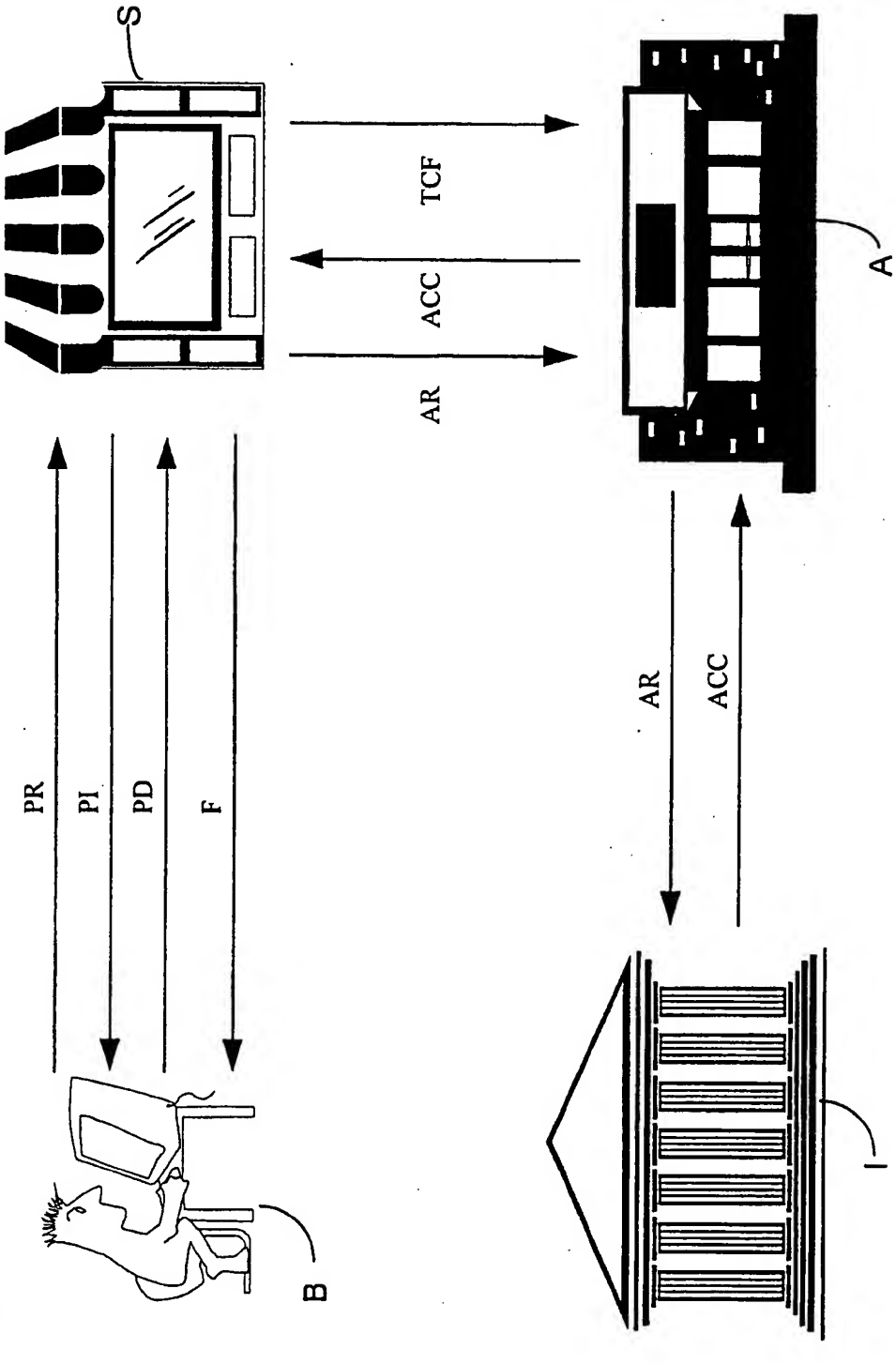


Fig. 1

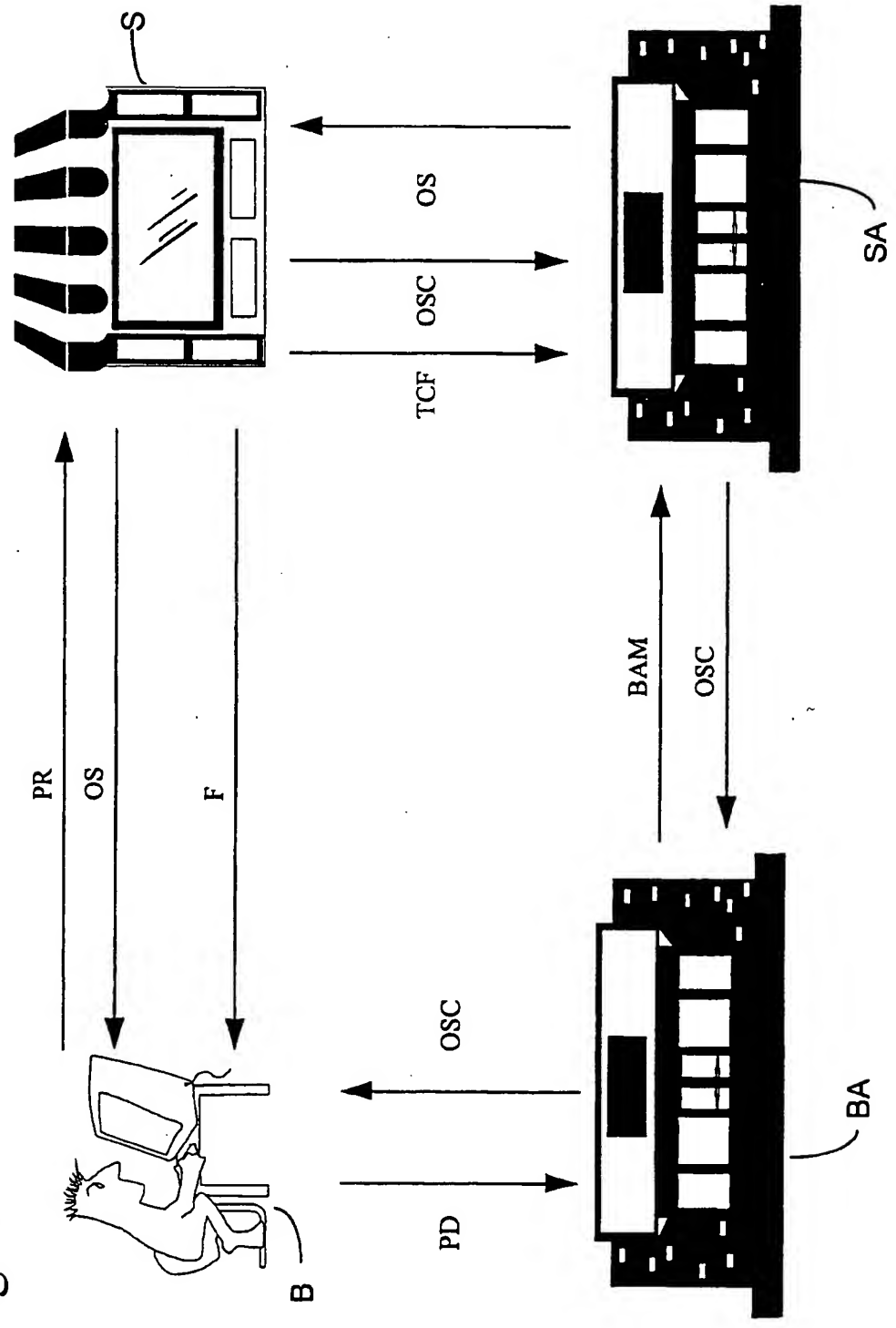


Fig. 2

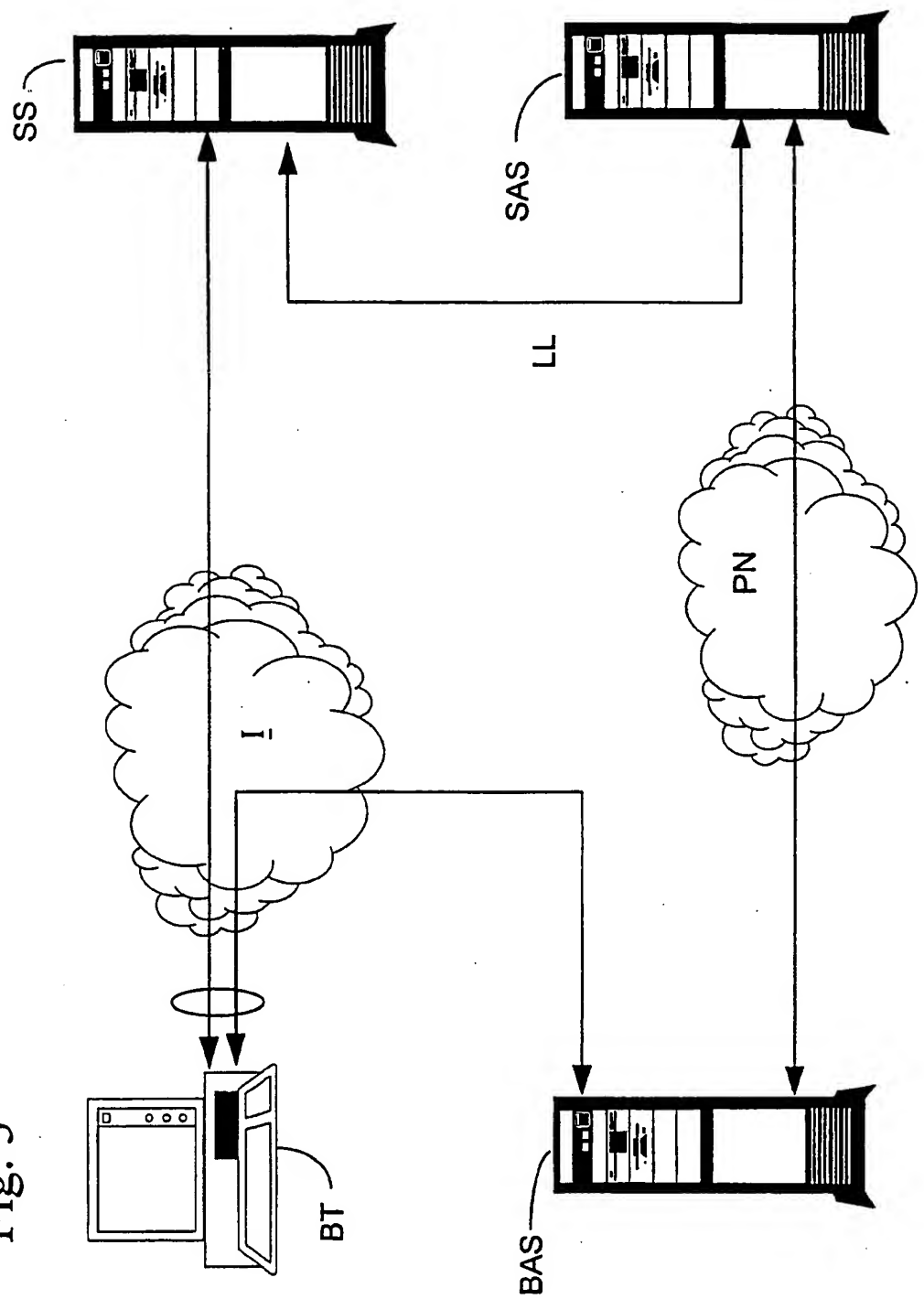


Fig. 3

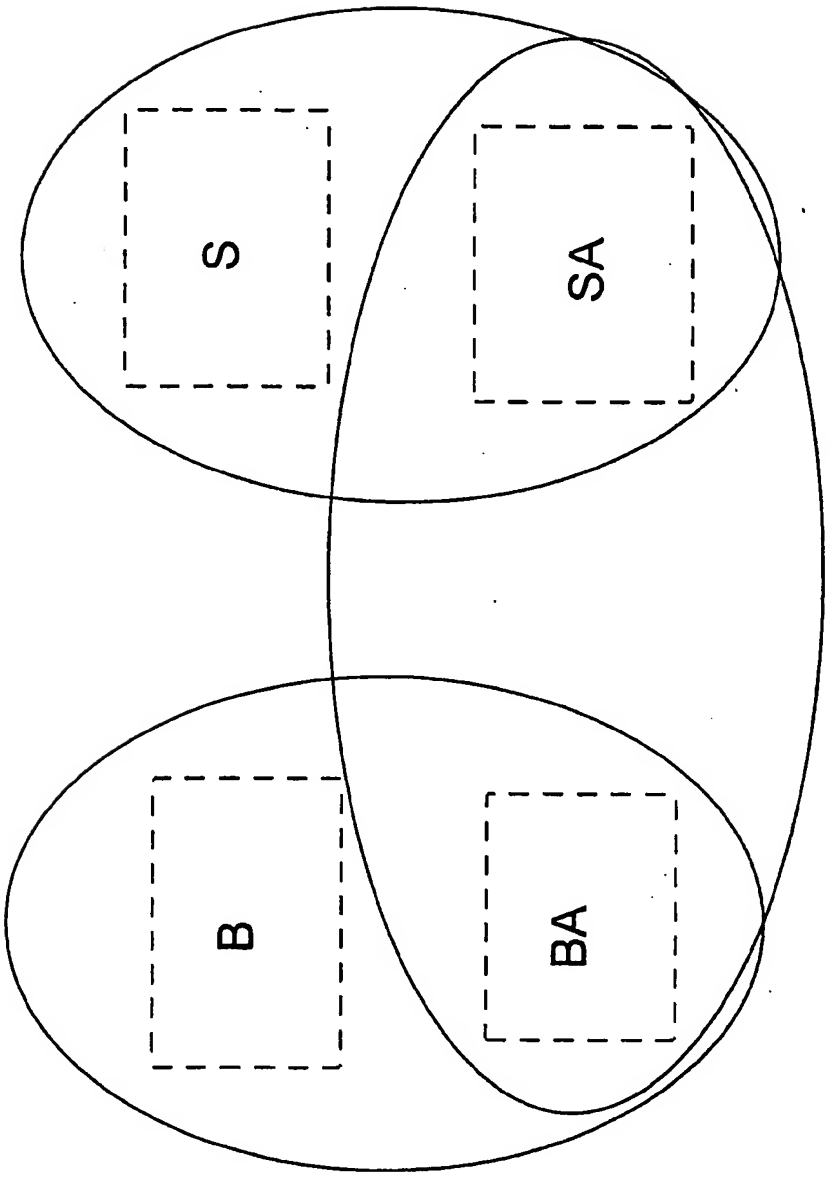


Fig. 4

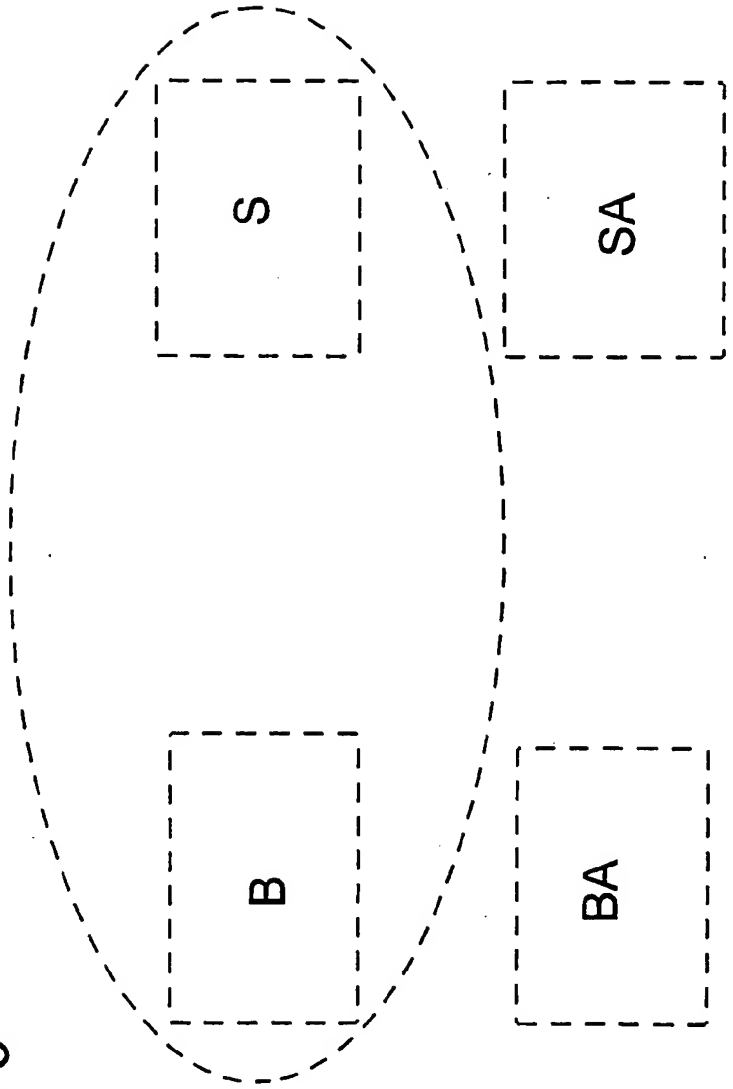


Fig. 5

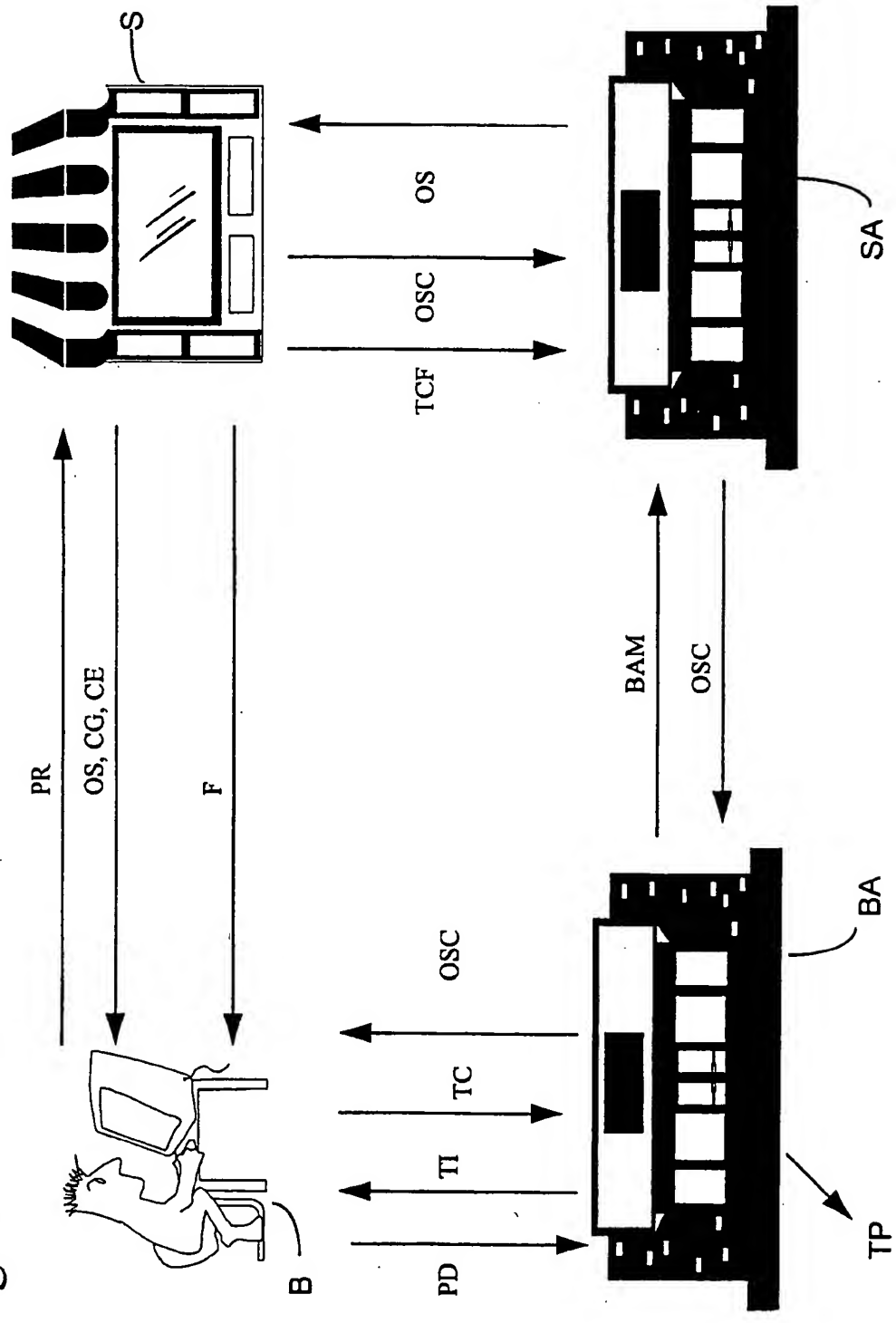


Fig. 6

INTERNATIONAL SEARCH REPORT

Interna..nal Application No
PCT/GB 99/02017

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F19/00 G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 793 028 A (C.S. WAGENER) 11 August 1998 (1998-08-11)	1-3
A	abstract; claims; figure 1 column 4, line 31 -column 13, line 62	5-7, 25-33
A	US 5 420 405 A (N.E. CHASEK) 30 May 1995 (1995-05-30) abstract; claims; figures column 1, line 40 -column 2, line 51 column 7, line 37 -column 8, line 13	1,2,4-6, 8-13, 16-33
A	WO 96 31965 A (FINANCIAL SERVICES TECHNOLOGY CONSORTIUM) 10 October 1996 (1996-10-10) abstract; claims; figure 3 page 14, line 17 -page 17, line 7	1,8-16

-/—

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 March 2000	03/04/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	David, J

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Intern. ial Application No
PCT/GB 99/02017

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE 196 28 045 A (ESD INFORMATION TECHNOLOGY ENTWICKLUNG) 22 January 1998 (1998-01-22) abstract; claims; figures	1-16
A	EP 0 807 910 A (NIPPON TELEGRAPH AND TELEPHONE) 19 November 1997 (1997-11-19)	
A	US 5 809 144 A (M.A. SIRBU) 15 September 1998 (1998-09-15)	
A	WO 99 23617 A (G. KREMER) 14 May 1999 (1999-05-14)	

INTERNATIONAL SEARCH REPORT

Information on patent family members

Interna al Application No
PCT/GB 99/02017

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5793028 A	11-08-1998	NONE	
US 5420405 A	30-05-1995	NONE	
WO 9631965 A	10-10-1996	US 5677955 A	14-10-1997
		BR 9608448 A	07-12-1999
		CA 2217593 A	10-10-1996
		EP 0819345 A	21-01-1998
		JP 11503541 T	26-03-1999
DE 19628045 A	22-01-1998	NONE	
EP 0807910 A	19-11-1997	JP 10083426 A	31-03-1998
		US 6003765 A	21-12-1999
US 5809144 A	15-09-1998	NONE	
WO 9923617 A	14-05-1999	FR 2771875 A	04-06-1999
		AU 1158899 A	24-05-1999